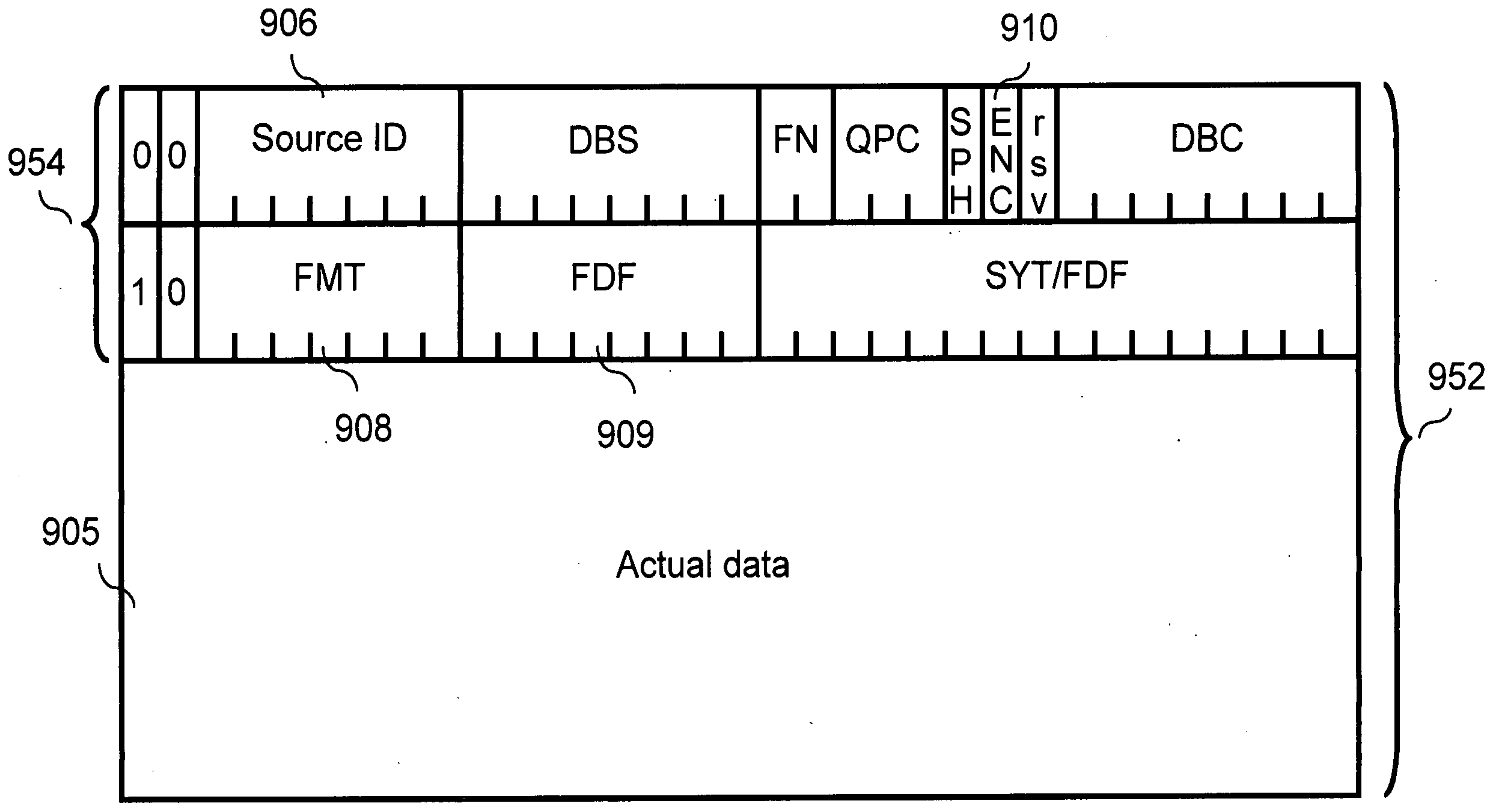
906
910
954
0
0
Source ID
DBS
FN
QPC
SPH
ENC
rsv
DBC
1
0
FMT
FDF
SYT/FDF
952
908
909
905
Actual data

FIG. 1

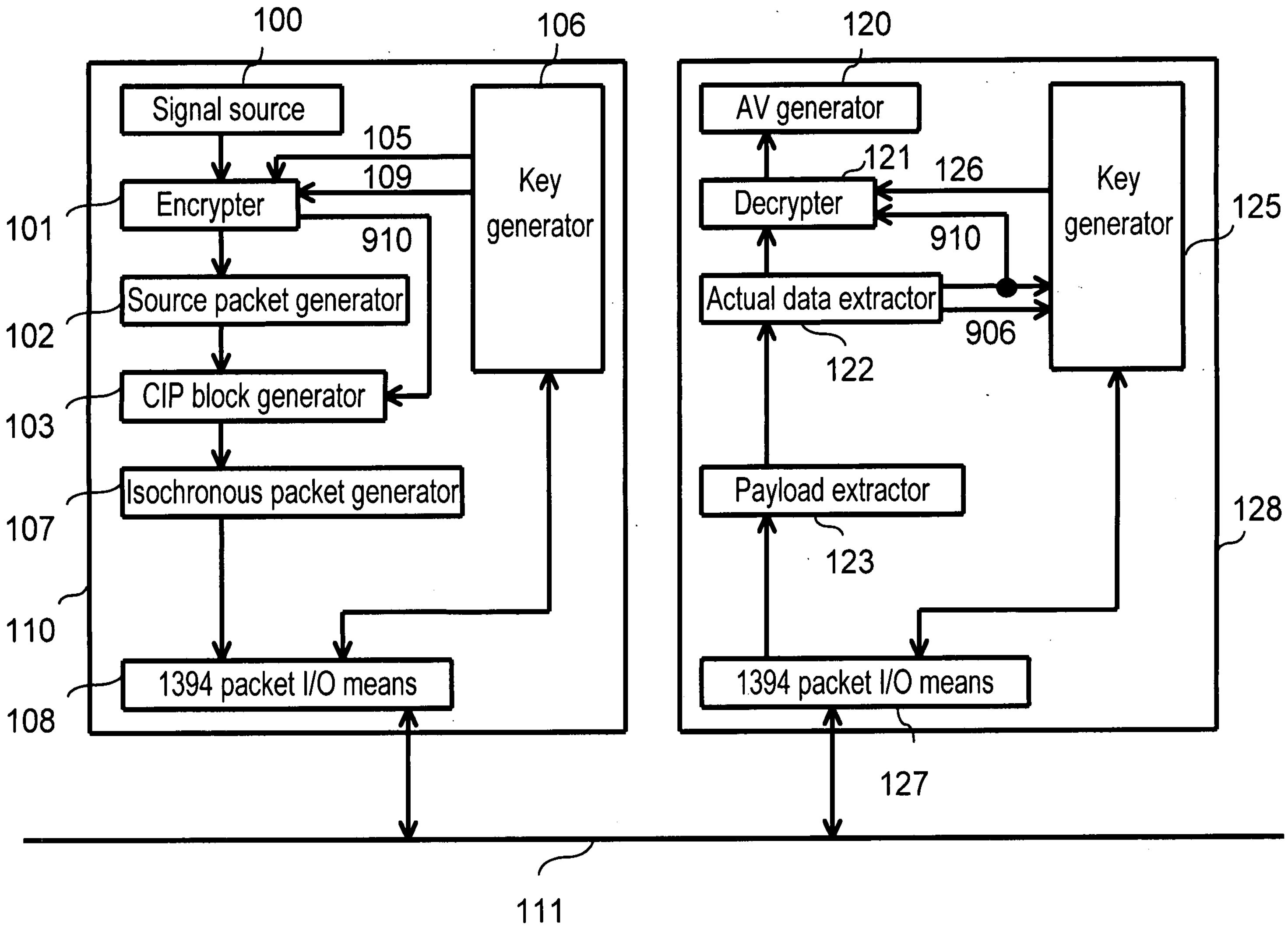
100
106
Signal source
105
109
Key generator
101
Encrypter
910
102
Source packet generator
103
CIP block generator
107
Isochronous packet generator
110
108
1394 packet I/O means
120
AV generator
121
126
Decrypter
910
Key generator
125
Actual data extractor
906
122
Payload extractor
123
128
1394 packet I/O means
127
111

FIG. 2

09/403560

FIG. 3A

208 operation code

	msb	lsb	
opcode	Authentication and Key exchange		
operand[0]	F_{15}	algorithm ID	200
operand[1]	FF_{16}		
operand[2]	FF_{16}		
operand[3]	FF_{16}		
operand[4]	FF_{16}		
operand[5]	FF_{16}		
operand[6]	FF_{16}		
operand[7]	FF_{16}		
operand[8]	FF_{16}		

FIG. 3B

208 operation code

	msb	lsb	
opcode	Authentication and Key exchange		
operand[0]	0	algorithm ID	200
operand[1] operand[2]	(msb) algorithm field (lsb)		201
operand[3]	FF_{16}		
operand[4]	FF_{16}		
operand[5]	FF_{16}		
operand[6]	FF_{16}		
operand[7] operand[8]	(msb) maximum data length (lsb)		212

FIG. 3C

208 Operation code

	msb	lsb	
opcode	Authentication and Key exchange		
operand[0]	reserved	algorithm ID	200
operand[1] operand[2]	(msb) algorithm field (lsb)		201
operand[3]	label 202	step No.	203
operand[4]	subfunction		299
operand[5]	channel No.		204
operand[6]	block No. 205	total block No.	206
operand[7] operand[8]	(msb) data_length (lsb)		209
operand[9] : operand[8+ data_length]	data		207

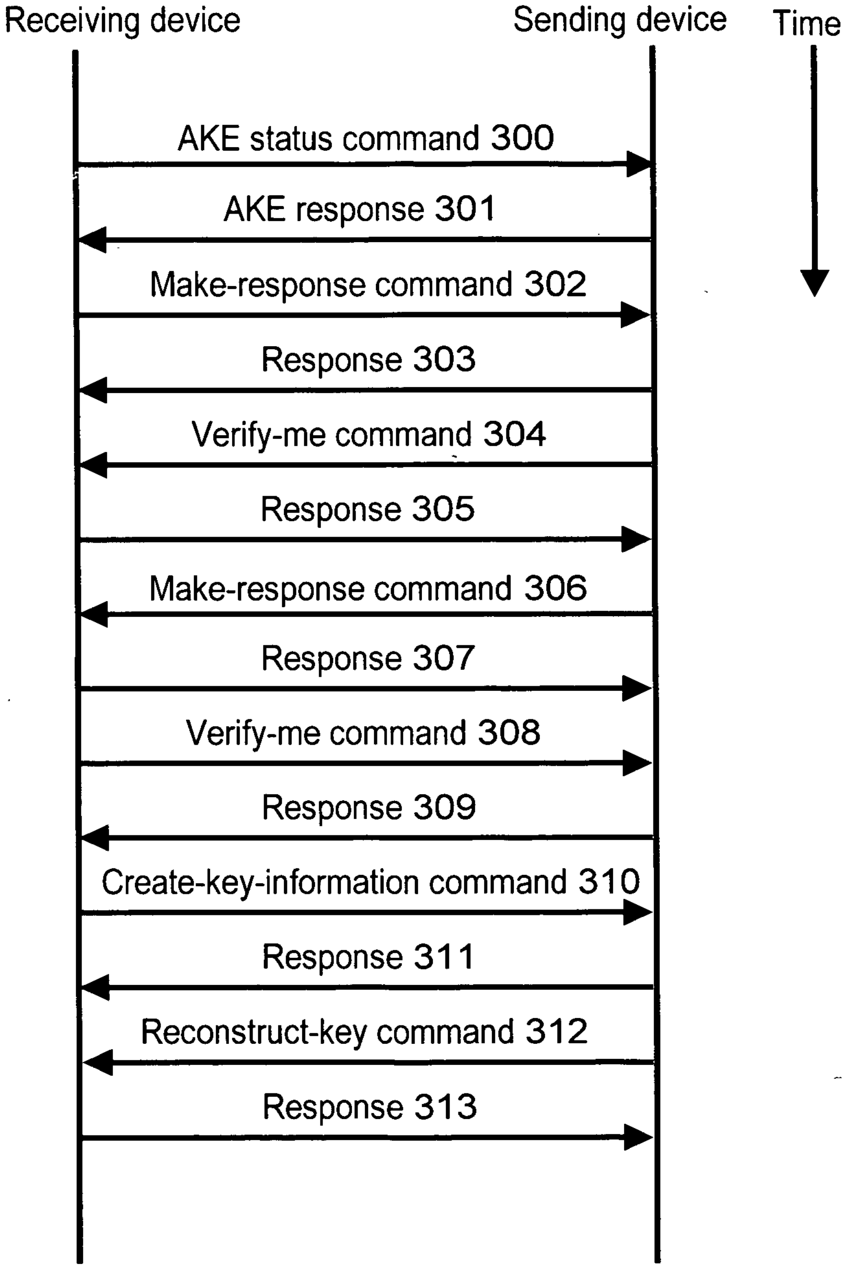
Receiving device
Sending device
Time
AKE status command 300
AKE response 301
Make-response command 302
Response 303
Verify-me command 304
Response 305
Make-response command 306
Response 307
Verify-me command 308
Response 309
Create-key-information command 310
Response 311
Reconstruct-key command 312
Response 313

FIG. 4

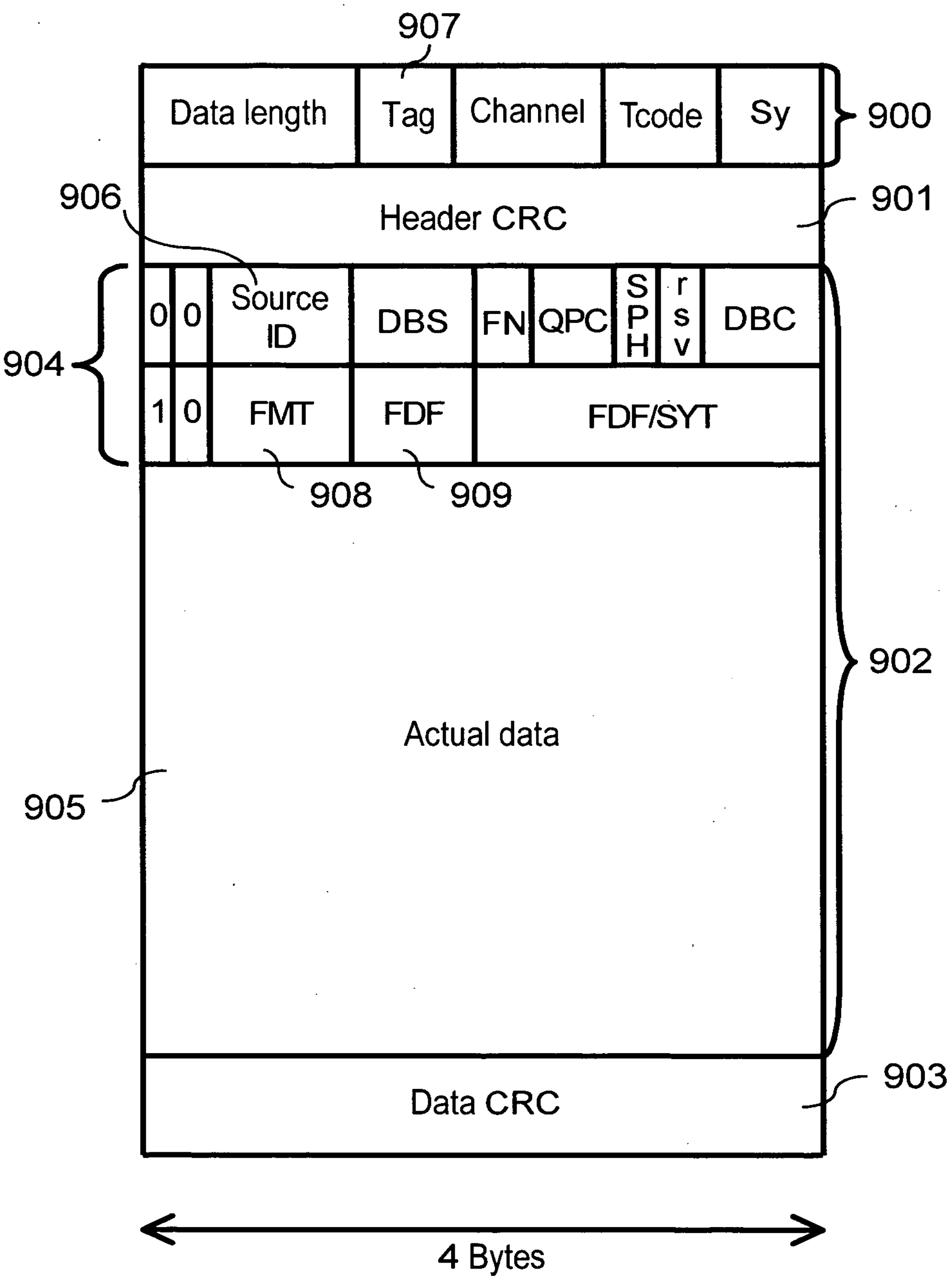

FIG. 5 PRIOR ART

Reference numerals

100	signal source
101	encrypter
102	source packet generator
103	CIP block generator
107	isochronous packet generator
108, 127	1394 packet I/O means
105	output command
109, 126	encryption key
110	sending device
128	receiving device
111	IEEE 1394 bus
106, 125	key generator
120	AV generator
121	decrypter
122	actual data extractor
123	payload extractor
200	algorithm ID
201	algorithm field
202	label
203	step No.
204	channel No.
205	block No.
206	total block No.
207	data
208	operation code

209	data length
212	maximum data length
299	subfunction
300	AKE status command
301	AKE response
302, 306	make-response command
303, 305, 307, 309, 311, 313	response
304, 308	verify-me command
310	create-key-information command
312	reconstruct-key command
900	isochronous packet header
901	header CRC
902, 952	isochronous payload
903	data CRC
904, 954	CIP header
905	actual data
906	source ID
907	tag
908	FMT
909	FDF
910	encrypting information (ENC)
952	isochronous payload